Abubakr Abdulgadir

Project Specification

High-speed Implementation of Authenticated Ciphers Competing in the CAESAR Contest

Motivation

Digital system designers are always trying to design faster implementations to keep up with the demand for more powerful computing systems. Authenticated ciphers combine the goals of confidentiality and authentication in a single algorithm. Speed or throughput of authenticated cipher is one of the most important criteria in evaluating these ciphers.

Implementation and testing tools

Design entry method will be RTL VHDL. Targeted platform is Virtix6. Xilinx ISE will be used to design the circuit.

The GMU hardware API will be used as a hardware interface and the system will be implemented and simulated as VHDL code.

This project will use the existing GMU Hardware API as a platform for testing the circuit and GMU VHDL implementation of AES may also be used as a building block in the circuit.

The specification of the implemented cipher is provided in [1]. Also the reference C implementation of the Deoxys cipher from the SUPERCOP package will be used for clear understanding of the cipher.

Testing will be done using Xilinx ISE simulator ISim and test vectors will be generated using the python script from the GMU Hardware API support files.

Tests will be done by operating the circuit with various message sizes. The parameters of interest in the testing phase will be throughput for long messages and execution time for short messages.

Goals

The design target is to implement the Deoxys CAESER candidate with the hardware optimized for speed.

Speed will be measures by throughput in Megabits per second for long messages and execution time for short messages in nanoseconds.

Timeline

Oct 14: Final project specification.

Oct 21: Understand the tools used to implement the project and high level design of the circuit.

Nov 4: Implementing individual circuit components.

Nov 18: Integrating circuit component and testing.

Dec 2: Testing and evaluation of target metrics.

Final report tentative table of content:

-Abstract

-Introduction

-Motivation

-High level design and optimizations

-Circuit implementation

-Testing and results

-Conclusion

Literature

1- Jeremy Jean, Ivica Nikolic, Thomas Peryrin, “Deoxys v1.3” in DIAC 2014, Santa Barbara, CA, 2014, pp. 2-12

2- E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M.U. Sharif, and K. Gaj "GMU Hardware API for Authenticated Ciphers," GMU, Fairfax, VA, Rep 2015/669, Jul

3- M. Liberatori, F. Otero, J. C. Bonadero, J, Castifieira, "AES-128 cipher. High speed, low cost FPGA implementation," in Prog. Log. Conf., Mar del Plata, 2007, pp. 1-4